Crime Science
a SpringerOpen Journal

THEORETICAL ARTICLE Open Access

Developing an alternative formulation of SCP principles – the Ds (11 and counting)

Paul Ekblom[1*] and Alexander Hirschfield[2]

Abstract

Background: The 25 Techniques of Situational Crime Prevention remain one of the bedrocks of research in Crime Science and play a key role in managing knowledge of research and practice. But they are not the only way of organising, transferring and applying this knowledge.

Discussion: Taking the 25 Techniques and their theoretical underpinnings as our starting point, this paper presents the (currently) 11 Ds, a set of intervention *principles* which focus specifically on how the interventions are intended to influence the offender in the proximal crime situation. The context of this work was a project to help security managers detect and control attempts to undertake 'hostile reconnaissance' of public places by those planning to commit crimes or acts of terrorism. We discuss why we judged 25 Techniques as a model for emulation in general terms but unsuitable in detail for the present purpose. We also describe the process of developing the principles, which involved both reflection, and capture of new knowledge from theory and practice, including the security domain. The distinctive contribution of professional design to this process is noted. We then present the Ds themselves and show how, as generic principles, they relate to practical methods of prevention; how they can be further organised to aid their learning and their use; how they relate to other formulations such as the Conjunction of Criminal Opportunity; and how they might apply, with expansion perhaps, to the wider field of SCP.

Summary: We discuss the process and the wider benefits of developing alternative – but rigorously linked – perspectives on the same theories and phenomena both for transferring existing research knowledge to practice and for sparking leading-edge theory and research.

Keywords: Situational crime prevention; Problem-oriented policing; 25 Techniques; Design; Crime science; Knowledge management; Practice; Crime scripts; Deterrence

Background

Situational Crime Prevention (SCP, see Clarke 2008) and Problem-Oriented Policing (Scott et al. 2008) are major defining domains within Crime Science (e.g. Laycock 2005). Overall, Crime Science aims to constitute the hub of rigorous research and theory applied to the practice of reducing the risk of criminal events. Risk in turn covers the possibility of undesired criminal (and related) events happening at all, the probability of their occurrence and the harmful consequences that may follow (e.g. Ekblom 2012a).

Over the last three decades a large body of research and theory-based practice knowledge has accumulated, mostly accessible via the website of the Center for Problem-Oriented Policing. There are various core organising elements of this knowledge:

- An 'action-research' model of the preventive process, SARA (Scanning, Analysis, Response, Assessment);
- A basic model of the proximal causation of criminal events, and guide to the mechanisms or principles of preventive interventions, the Problem Analysis Triangle (PAT, formerly Crime Triangle);
- A structured and cumulative catalogue of practical preventive methods, the 25 Techniques of SCP (25 T);
- Various crime-type specific empirical assemblages of risk and protective factors, more associated with the offence than the offender, characterising particular

* Correspondence: p.ekblom@csm.arts.ac.uk
[1]Design Against Crime Research Centre, Central Saint Martins, University of the Arts London, Granary Square, London N1C 4AA, UK
Full list of author information is available at the end of the article

crime targets e.g. the CRAVED properties of 'hot products' (Concealable, Removable, Available, Valuable, Enjoyable, Disposable) (Clarke 1999) and terrorism-related target selection factors (EVIL DONE: Clarke and Newman 2006);
- A process language, crime scripts (Cornish 1994) for describing the sequential aspects of criminal events and related behaviour.

These frameworks, thoroughly described in Clarke and Eck (2003) and Wortley and Mazerrolle (2008), relate to underlying theories/perspectives. For example PAT, centring on Offender, Target/Victim and Place, is close to the Routine Activities triad of Offender, Target and Guardian (Cohen and Felson 1979) especially when the triangle is embellished with its outer 'crime preventer' roles of guardians, managers and handlers). The 25 T were originally organised exclusively in terms of the offender's Rational Choice 'opportunity' agenda (Cornish and Clarke 1986) of risk, effort and reward. Later were added two ad hoc principles of removing excuses and controlling provocations, the latter reflecting 'crime precipitation' theory (Wortley 2008). This describes a two-stage process of causation of criminal events, with situational determination of opportunity preceded by situational arousing or releasing of motivation (permissions, prompts, provocations and pressures).

Partial competitors exist to SARA (e.g. 5Is, a more detailed equivalent with major task streams of Intelligence, Intervention, Implementation, Involvement and Impact: see Ekblom 2011) and PAT (e.g. Conjunction of Criminal Opportunity, with causation of criminal events differentiated into 11 elements, and counterpart intervention principles: see Ekblom 2010, 2011). These evolved from a critique of limitations of the familiar frameworks, addressing knowledge management concerns over consistency, integration and the ability to organise complex and detailed knowledge of practice. Whatever the ultimate resolution of such competition, the theme pursued in this paper is that the traditional frameworks are not the only ways of organising Crime Science knowledge for practice, research and theory. There are cases where it is both desirable and appropriate to manipulate, reconfigure and add to existing theoretical frameworks to generate principles and methods that can be applied to different and evolving crime and security threats.

In some ways we can consider our knowledge like a rough diamond: to get it to radiate, scintillate and stimulate in a multitude of ways, we occasionally need to cut and polish new facets into it, to afford us different views into the rich interior. One such facet is the Ds framework, for organising our knowledge and thinking about how preventive interventions work by influencing the offender.

Genesis of the Ds

The origins of the Ds framework were in contract work for the UK's Centre for Protection of National Infrastructure (CPNI). The project concerned the development of an interactive computer-based toolkit to help security managers of large, crowded or critical infrastructure sites to control hostile reconnaissance by perpetrators. This is the process whereby those with malintent strategically select sites that are desirable and feasible to attack, and simultaneously acquire tactical information. Underlying the toolkit was the rationale that if you control reconnaissance, you reduce the risk of main attack, whether by terrorists, armed robbers, industrial spies or protesters. The initial requirement was to incorporate ideas and approaches from SCP and POP, to widen the scope of the 'what works' knowledge drawn on, and to enrich the thinking of 'mainstream' security practitioners. This led ultimately to the toolkit, now under final user test on a secure website. A presentation (Willcocks et al. 2012) is available from the authors.

The paper proceeds as follows. We first describe the process of capturing client/user requirements for the hostile reconnaissance toolkit as a whole, and then cover what content-knowledge was gleaned from the security domain and from Crime Science. We next focus on the particular contribution from 25 T, and identify limitations for present purposes which led us to develop an alternative formulation centring on a greater number of principles and a lesser number of methods of control, and focusing more single-mindedly on influencing the offender. We set out these principles and methods and briefly relate user reactions. In the summary we report on the *process* of developing the framework – know-how that can be applied in evolving *other* facets for our knowledge as and when needed. We review the benefits to practitioners of using the method/principle distinction and the Ds in particular, and cover counterpart benefits to Crime Science. Finally we look ahead to further developments and consider some wider implications for Crime Science.

Discussion

The development of the toolkit involved a mixed team of crime scientists and designers, with close involvement of clients (CPNI and their colleagues) and end-users (security managers). Capturing client and user requirements was undertaken in step with reviewing literature from both the security world and that of SCP/POP to seek and then combine principles and practices which would, suitably organised and formulated, meet those requirements.

Capturing client/user requirements

Requirements capture supported considerations of both toolkit content and toolkit design. For the designers it

was important to determine what format(s) the toolkit should take; how it could fit best and prove most useful within users' existing patterns of work and routines on site; as well as informing what level and kinds of content should be presented, in order to produce a genuinely accessible, usable and valuable toolkit for these groups. The interview consultations and feedback were fed directly into multiple stages of the design process from the respective rounds of interview iterations. This, in turn, helped shape the definition and development of the toolkit concept designs, which were then shown and trialled for further feedback during consecutive stages.

Requirements capture involved a) initially five site visits to diverse venues including major rail stations, shopping malls and football stadium; and b) hour-long semi-structured interviews with 20 stakeholders comprising in roughly equal proportion government and police security advisers, and additional site security managers. People and sites were identified through a combination of recommendations by CPNI (who also vouched for our good intent) and prior local research contacts.

The site types and instances were chosen because they covered a diverse range of the kind of venues where action was required and where security managers, of sufficient experience and organisational authority/resourcing, were present and empowered to take that action. These sites were later supplemented by visits to industrial plants as the scope of the study was extended. Each visit comprised a tour of the site followed by mainly group interviews with relevant security personnel.

These interviews and the additional stakeholder interviews each ran for approximately one hour, and were conducted using a semi-structured questionnaire. The primary aim of the interviews with security managers was to gain an understanding of what the job involved, particularly in conducting surveillance at different types of site, to explore how far they worked in partnership with other agencies, their degree of autonomy in making decisions about security measures and to identify their awareness, knowledge and experience in recognising and responding to hostile reconnaissance. Of particular importance here, was how far they felt they had sufficient information to alert them to a possible attack, who to share this information with and what action to take under such circumstances. Questions probed their views on the need for appropriate guidance in such situations and the content, nature and format of any future guidance, particularly, the development of a web-based toolkit. Different toolkit design options were presented to the respondents towards the end of the interview. Interviews with official security advisers covered many of the same issues but also sought to better understand the advisory role, particularly the way in which advisors interacted and communicated with security managers, their views on how far hostile reconnaissance was a priority for security managers and the extent to which the latter complied with their advice.

We found that sites were highly varied (in terms of size, functions and layout), often individually complex (e.g. changes in usage and customer base by time of day) and with varied ownership and control over land. Employment practices on site, including the hiring and vetting of staff, were also subject to variation when site employees worked for different companies.

Security issues changed strongly over daily, weekly and monthly cycles depending on activities and closures. Security managers had extremely variable levels of knowledge and available time (some were general managers or engineers with add-on security responsibilities, others were specialists with a police/military background); and the kind of high-impact/low probability events in question were challenging to plan and to budget for.

The toolkit had to handle all these issues, bringing security, SCP and POP together in a way that was inclusive of ability levels, and generic across the diversity of venues. It had to focus on perpetrator actions and goals because security managers can never be quite sure of the specific nature of the criminal acts to be expected, hence are in no position to focus on a narrow set of threats[a]. It also needed to be generative, i.e. capable of producing a wide range of suggestions for action that were plausible in both scientific and practical terms; that offered versatility and 'design freedom' (Ekblom 2012a, b) for managers of all levels of sophistication working in diverse sites; and that gave them a mental schema to adjust knowledge of what works at theoretical/practical levels to their own working context. This last, respecting the strong context-dependence of what works, is considered central to effective crime prevention (Pawson and Tilley 1997; Ekblom 2011).

Learning from security

Rapid familiarisation with the conventional security literature yielded rather thin pickings. Terminologically, the interventions came under two generic headings – deter and detect and that was largely it. For a discipline purporting to influence a wide range of human misbehaviour, this was disappointingly limited, although we concede a more thorough investigation might have yielded more. More interesting was an encounter with Effects-Based Operations e.g. Batschelet (2002): this is a process, military in origin, of careful identification of one's adversary's strategic and tactical goals, followed by assembling a combination of highly-focused efforts to try to block them.

What did Crime Science offer?

Traditional Crime Science frameworks similarly revealed limitations in what they could offer. PAT in fact took us

little further than existing security knowledge, although the latter's language was rather different, less consistent and less analytic. Risk-factor approaches such as EVIL DONE (for identifying targets at risk of terrorist attack – Clarke and Newman 2006) were useful elsewhere in the toolkit (under 'think opportunity'). SARA, having evolved as a process for identifying and responding to empirical risk patterns in what are often open-ended collections of sites, was not particularly adapted to assessing risks of a known category of malicious behaviour in a known site. Although the toolkit itself did require a process model to take the user through the action steps, we drew on a wider range of sources than SARA, including 5Is; but this is not the focus of the present article (Willcocks and Ekblom 2012 give some impression).

We reached the working position that the only common organising factors behind helping security managers understand and control hostile reconnaissance in diverse sites, and diverse situations within these, were *what the perpetrator is trying to do and how*. So we decided to centre our ideas for the toolkit initially on what the perpetrator is trying to achieve (effects), how (scripts), and then flip to how the security team might anticipate, recognise and control this (interventions). (The full sequence in the toolkit can be described as 'think perpetrator', 'think opportunity', 'think intervention', think designer' and 'think manager'). For this purpose 25 T looked a more promising start.

The 25 techniques

We looked at the 25 T at various levels (readers are recommended to consult the diagram at the Center for Problem-Oriented Policing website www.popcenter.org/25techniques/): what we termed *principle*s (the five columns of increase the effort of offending, increase risks, reduce rewards, reduce provocations and remove excuses); the *method category* level (the 25 cells, e.g. 'remove targets'); and the *method exemplar* level (i.e. the specific instances of action listed under each category, e.g. 'removable car radio', 'women's refuges').

We did try to populate a 25 T table with hostile-reconnaissance-relevant exemplars of our own invention, but the results did not take us very far. Considering ourselves in effect as stand-ins for users, the experience indicated that a more radical approach was needed to stimulate the envisaging of a wide range of context- and problem-appropriate solutions. Our next move was thus to attempt to identify how far the 25Ts were helpful for our present purposes:

- Not all principles – e.g. *provocation* – appeared immediately suitable for addressing hostile reconnaissance (our immediate project goal, though beyond this, provocation makes a comeback as will be seen).
- The principles were rather too broad in their connection with underlying causal mechanisms – too few to handle the variety of intervention mechanisms we judged to be important.
- There is a concern (e.g. Ekblom and Sidebottom 2008) that the 'risk, effort and reward' principles are 'interchangeable currency' in that increasing the effort, say, may cause the perpetrator to tolerate greater risk if the reward is large enough, implying that the intervention principle *intended* may not be the one that is ultimately *delivered* or that adaptive and motivated perpetrators may adjust to it; also that risk, effort and reward cannot be seen as factors in isolation to be considered one at a time but part of a *holistic decision agenda*.
- The method category content within each of the principle columns comprise rather ad hoc assemblages of techniques, adequate for a very general-purpose knowledge bank but perhaps not for a highly-focused project as at present.
- Many method categories were already known to security: e.g. *Control Access.* Not all categories seemed suitable for highly motivated perpetrators: e.g. *making compliance easier.*
- Few existing exemplars leapt out at us as relevant, novel to security and transferrable.

If not 25 T for this project, then where next?

Beyond the 25 techniques

Moving on from the 25 T involved a fairly explicit exercise in design. We wanted to:

- Retain the *principles/method-categories/method-exemplars* structure of the 25 T (and incidentally also of 5Is) as we considered this fundamentally a good way of organising practice knowledge (we set out the benefits of principles below);
- Therefore ensure that principles and methods were distinct, offering perspectives that were alternative, not superior/inferior;
- Link principles more clearly to causal mechanisms, which are at the heart of the Scientific Realist approach to evaluation and transfer of its results to practice (Tilley 1993a, b; Pawson and Tilley 1997; Ekblom 2002, 2011; Wikström 2007);
- Tie the principles to the 'think perpetrator' approach, and focus consistently on the final common causal pathway of the offender (unlike 25 T which ranged between situation and offender);
- Link method categories more firmly to method exemplars in the form of 'practical actions that the security manager users could take';

- Wherever possible, maintain continuity of terms/concepts with 25 T.

We also wanted to produce material both applicable to our diverse scenarios and versatile, with an eye to utility beyond this project.

The result was a *wider* range of control principles than in 25 T and a *narrower* range of generic control method categories; this allowed for a fully open-ended set of specific practical actions rather than a limited set of method exemplars. (We also shifted terminology from 'prevention' to 'control' on the grounds that not all the actions against reconnaissance would be preventive in the sense of preceding the criminal event. Another terminological move was to substitute 'perpetrator' for 'offender' to fit better with security/counter-terrorist literature and the inability to find a more specific term: 'hostile reconnaisseur' was contemplated, but not for long).

The principles and methods finally adopted were the outcome of intensive reflection and debate among the research team, with the clients and with users in the many iterations of designing and improving the content, language and structure of the toolkit over the course of several months. This process involved group feedback sessions with the client's staff and other security experts, in which extensive notes were taken and systematically incorporated in the next iteration; single user workshop trials (where each practitioner was first observed working through the toolkit with no additional prompts or designer-initiated questions, and then taken through again with active prompts and queries about content, navigation etc.); and four brief field trials which involved visiting individual security managers, and taking them through the toolkit applied to a real-life zone within their own site. The sites included a major City of London office block, a large Yorkshire railway station and a chemical plant in Greater Manchester.

Control methods

The control methods we defined, being tangible and practical, were fairly straightforward to determine. They derived variously from category headings and exemplars of 25 T; from numerous security practice guides; and from picking the brains of the security advisers and end-users involved in the requirements capture and trial iteration stages. We were careful, too, to focus users at this point on methods of *intervention* (i.e. those that intervened in the causes of the criminal or terrorist events) rather than methods of *implementation* or of *involvement*, a distinction introduced in the 5Is framework, differentiating the 'Response' stage of SARA.

The list of basic control methods that emerged was surprisingly brief:

- Access control;
- Exit control;
- Constraining specific movement and behaviour (of perpetrator and other users, for example forbidding photography);
- Surveillance (and consequent action e.g. targeted challenge);
- Security escort (close accompaniment of visitors around the site);
- Random confrontations/challenges;
- Information/misinformation (for example highlighting/exaggerating 'new security measures' of unknown type on the venue's website, and removing views helpful for reconnaissance; or 'decoy' techniques to differentially attract perpetrators to particular locations such as spuriously labelled 'secure areas', thereby making them self-reveal their intentions when they loiter there).

Control principles

Pinning down what we meant by the 'principles' was somewhat harder. Only after persistent contemplation did their nature become explicit. Here we should note the contribution of the information/communications designers in the team, whose graphic reflections of what we were fumbling towards greatly aided the articulation process.

The defining nature of the principles that emerged was *how the interventions are intended to influence the offender in the proximal crime situation.*

This enabled us, say, to distinguish between 'supply information/misinformation' as a method, and 'deceive perpetrators' as a principle. Generally principle and method were linked through a 'by' sentence: 'Deceive perpetrators *by* misinformation'… 'Defeat perpetrators *by* controlling movement and behaviour'.

The principles that resulted came from diverse sources including principles, categories and exemplars of 25 T, security practice and the Conjunction of Criminal Opportunity.

- 'Deter' obviously pre-existed in the security world but with the loose meaning of 'anything that puts the perpetrator off'. The Rational Choice agenda and its manifestation in the 25 T principles yielded the more precise *Deter* (increase perceived risk) and *Discourage* (increase perceived effort, reduce perceived reward: see also Felson 1995). Reflecting discussions with clients/users we decided to split deter into *Deter-known* and *Deter-unknown*, given the latter was claimed to convey distinctly different, and stronger, influences on perpetrators.
- Physical blocking, *Defeat/Delay*, originated from a combination of target hardening (25 T) and creating target enclosure (CCO).

- Deflecting offenders in 25 T, combined with offender presence in CCO, plus security 'decoy' attractions (described above) led to *Deflect from/Direct to.*
- Enforcement actions of *Detect* and *Detain* took the principles beyond normal SCP though *perception* of these give force to deterrence, and remove offender presence (as in Routine Activities and CCO).
- Control tools/weapons (25 T) and the more generic restrict resources for offending (CCO) led to *Disable/Deny*, covering two distinct but linked aspects, as with blocking wireless signals and confiscating camera phones.
- Alert conscience (25 T) and the more generic readiness to offend (CCO) yielded *Demotivate* (since this applies to SCP we are here talking about proximal, situational influences on motivation like pictures of families at risk of harm, not distal ones like radicalisation).
- As a precipitation process (Wortley 2008) that aids preventers to detect and deter more than provoking perpetrators to offend, we identified *Disconcert*. The idea was suggested during a trial iteration of the toolkit, by the security manager of a large London multiplex concert venue. Queuing concert-goers would shuffle along complex paths en route to particular events, and the security staff would randomly reposition metal-detecting arches along the way. The upshot was that perpetrators carrying knives, when rounding a corner and being confronted with the unexpected sight of an arch, would often show a startle response, leading them to self-reveal to watching security staff, or to be sufficiently 'spooked' to dispose of the weapon or turn back. Interestingly, this knowledge capture episode shows how the toolkit trial process was not only necessary for design improvements, but also constituted a means of extracting fresh practice knowledge.

The generic definition and specific elaboration of the above principles for controlling hostile reconnaissance largely maintains the SCP focus on the offender's view of the situation. But although opportunity reduction makes a major contribution, motivational/emotional factors are included as per Wortley's (2008) precipitators and the CCO. In this, we adopt the 'caused agent' perspective identified by Ekblom (2012a) whereby the offender's behaviour is seen as both situationally *caused* (by provocations and other motivating factors) and *causing* of criminal or terrorist events (via active taking of decisions and pursuit of goals and plans).

Principles may act in chains: for example, Deceit about risks of being caught can feed Deterrence. As noted elsewhere (Tilley 1993b, Ekblom 2011) there was often a many-to-many relationship between principle and method. For example, Discourage could be delivered by the increased effort of circumventing Access Control, or Misinformation in the form of the disguising of rewarding targets. And Access Control, in turn, could activate the principles of Discouragement, Deterrence-known and -unknown, Detect and Detain. Recall, also, the 'interchangeable currency' issue in the rational choice agenda discussed above, meaning that activating one principle may perturb the wider system which could require users holistically to consider pinning down other principles simultaneously (e.g. in terms of the 25 T principles, simultaneously increasing risk *and* effort; in 11D terms, Deter *and* Discourage).

The D principles – how the interventions are intended to influence the offender in the proximal crime situation – are summarised as follows.

- Defeat: physically block access and movement or block/obscure the information that offenders want to collect
- Disable/Deny: equipment helpful to offenders such as bugs or cameras
- Direct/Deflect: offenders towards/away from place or behaviour
- Deter-known: offenders know what the risk of exposure is, and judge it unacceptable so abandon/abort HR attempt
- Deter-unknown: offenders uncertain what control methods they are up against, so again judge risk of exposure unacceptable
- Discourage: offenders perceive effort too great, reward too little, relative to risk, so abandon/abort attempt
- Demotivate: awakening, within offenders, motives/emotions contrary to the mission, e.g. empathy with potential victims, removing excuses, coward image
- Deceive: offenders act on wrong information on risk, effort, reward, where to go etc., and are exposed to immediate arrest or protracted intelligence collection, frustrated, or mistakenly decide not to select this site as target
- Disconcert: causing offenders to make overt involuntary movement or otherwise become startled
- Detect: passive, and active exposure to make offenders self-expose by instrumental, expressive or involuntary action; by making legitimate presence/behaviour distinctive; and by improving capacity of people exercising security role to detect
- Detain: once offenders detected, they must be caught and held (or credible identifying details obtained so they can be traced)

Principles: Taming the variety

Eleven principles are considerably more for practitioners to take in than the five of 25 T. We therefore sought to

cluster this diversity into fewer superordinate groups. This was a struggle: it proved impossible to derive exclusive supercategories, but eventually we identified three overarching analytic modes of action:

- Practical: limiting what perpetrators can do by changing the environment and its contents;
- Psychological: changing how perpetrators see, think or feel;
- Personal: spotting, identifying, catching, tracking or tracing the perpetrators.

A given principle could reflect one, two or all three of these modes (allowing licence for the 'interchangeable currency' issue already described). Thus for example Defeat/Delay are predominantly practical; Deceive and Demotivate predominantly psychological; Detain and Detect predominantly personal. Discourage is practical and psychological, and the Deter principles are simultaneously practical, psychological and personal (the perpetrator could, say, perceive and respond to the risk of detection and arrest from the physical barriers, detectors and procedures of strong access control arrangements). The full connections are in Figure 1.

Beyond principles and methods

Although the focus of this article is on the principles, it is important to see how these are intended to be applied in the complete toolkit cycle. Users are initially required to 'think perpetrator' in terms of particular, focused 'script scenarios' relating to specific user-defined zones of the site (such as 'tackling perpetrator *entering* site *control room*, pursuing goals of *obtaining strategic information on target* whilst *avoiding detection*). Having identified opportunities for reconnaissance at the site users are taken through the principles and methods, and essentially allowed to follow their preference in choosing and customising particular interventions stimulated primarily via the one or the other. They are, however, required at this stage to select one method at a time, and are then supplied with a range of method-specific exemplars to help them generate their own control actions.

In contrast to the abstractions of high-level principles and generic control methods of intervention, the actions they are now prompted to suggest are concrete *operational* or *preparatory tasks* to make the current method happen; and specific *people* to undertake them. (This reflects a subdivision of 'Response' in the SARA process, advocated in the 5Is framework (Ekblom 2011). Intervention covers, say, the operational action of searching visitors' bags for cameras. Implementation concerns the practicalities of preparatory tasks, such as installing tables for the search. Involvement includes for example internal security campaigns, where the professional preventers seek to mobilise employees to remember to search every time, and thoroughly.) In this way a collection of *actions* and relevant *responsible people* (security staff, other employees, trainers etc.) is built up to cover different perpetrator script scenarios employing a diversity of methods and covering a range of different zones of the site.

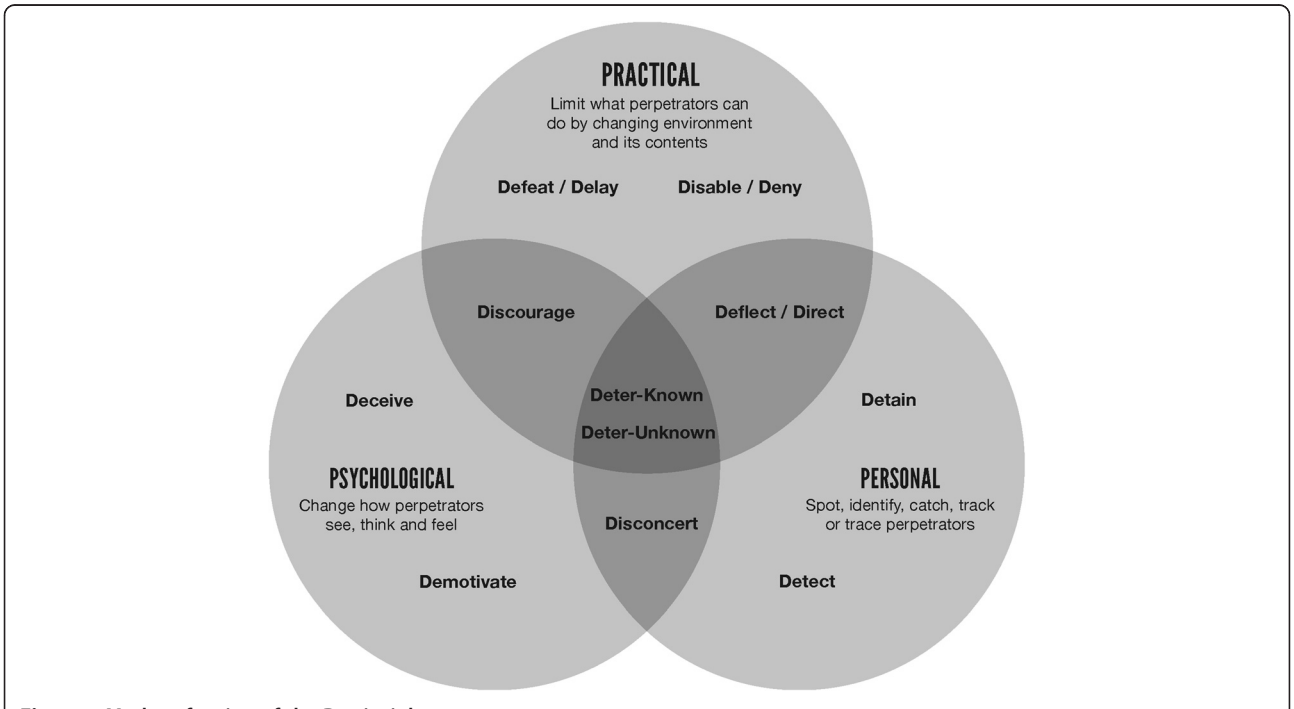

Figure 1 Modes of action of the D principles.

These tasks are then reviewed from a *design* angle, in which the users are prompted to shift perspective from 'security obsession' to additionally consider their suggested actions from wider viewpoints: mainstream business needs (e.g. profit and reputation); other security needs (not interfering with other security tasks); societal needs (e.g. inclusivity, health and safety); and user needs (e.g. hassle-free visiting). Users are also encouraged to consider wider operational requirements including cost, staff capacity and avoiding role conflicts.

Finally, the suite of actions is considered from a *management* perspective, as work to be approved and resourced by top management, and systematically implemented, reviewed, adjusted and improved.

Initial client and user reactions

We were conscious of our clients' understandable interest in simplification. However, the shared experience of workshops, visits and interviews carried them with us, in acknowledging the help users required to handle the often inescapable complexity of their sites and the focus and differentiation needed to address the security issues. These developmental iterations revealed, moreover, that right from the start practitioners at all levels grasped the principles/methods distinction. They also appreciated the mix of recipe and flexibility, and being made and helped to *think* rather than slavishly following checklists. In fact, many security managers wanted to rush off and apply the toolkit, and to use it in ways that had not been anticipated, e.g. training staff. At the time of writing, the toolkit is on limited release for several months of formal testing, after which final adjustments will be made.

Summary

We can draw conclusions from this work at several levels, ranging from the contributions of design to the benefits for practice and for crime science. But we begin with next steps with the Ds.

Where next with the Ds?

Although we do not anticipate that the D principles will expand in number very much, we regard them as 'work-in-progress': further candidates have already been suggested. Wortley (personal communication 2012) suggested that reducing provocation could be termed 'Dampening'; others of his situational precipitators are worth considering. 'Disrupting' of perpetrators' planned actions, leading to an aborted mission, is another possibility closely-related to the effects-based approach though this requires some further thinking through. The same applies to 'Derailing', whereby if things don't go according to plan, perpetrators are forced to think on their feet and improvise 'off-script', entering into unplanned and hence riskier and less effective behaviour rather than totally aborting their mission. Again, 'Distracting' might jeopardise performance of scripts and/or choice of tactical goals. And on another tack, subdividing principles such as Demotivate might lead to harvesting/differentiation of greater detail of practice, for example 'Disgust' – where, say, skunk sprays have halted assaults. We would encourage colleagues to suggest new or amended principles, although we may have to face up to running out of appropriate D words.

Although we reduced the number of control method *categories* to seven in this particular instance the number and nature of such categories is likely to differ between crime problems and/or contexts of application. Careful attention to the organisation of such categories, and rich illustration of individual exemplars, is important for effective knowledge capture and transfer.

Benefits to practitioners of using the principles/methods distinction

The principles/methods distinction adapted and taken forward in this project confers several benefits to crime prevention practice (see also Ekblom 2011; Tilley 2006):

- If users know how the control methods work upon perpetrators, they can better design practical solutions, monitor performance and consider improvements;
- Principles are generative, i.e. they can help users intelligently replicate (Tilley 1993a) and also innovate (Ekblom 2002), producing plausible fresh ideas for boundless new contexts or where no known methods yet exist; and help them keep up with adaptive offenders;
- Principles avoid users doing the minimum and simply 'designing down' to a fixed list;
- Principles are transferrable and organise practice knowledge.

One might think (a point suggested by a reviewer) that surely competent practitioners make this distinction as a matter of course? Our position is that training has to be suitable for less competent practitioners too; and that even for competent ones, *explicit* awareness and articulation of the different discourses available for thinking and communication (Ekblom 2012a) offers advantages over the tacit.

Benefits to practitioners of the D principles

The SCP literature acknowledges the *practical* primacy of principles and theory. Eck (2002), in a 'what works' context, states: '[the theories of situational prevention] do not dictate specific actions, but provide a framework for the creation of context- relevant interventions. In this example, the answer to the question, "what works?" to prevent crime at places is "routine activity theory and

situational crime prevention."' [2002:105]. We support the general spirit of this statement. However, we also note that as the Ds illustrate, such generic 'what works' principles can be further differentiated by mechanism tightly focused on a common theme (the nature of the causal influence of interventions on offenders). In our immediate experience, a diverse range of security practitioners and advisors appeared to understand and appreciate this approach.

In effect we are advocating a mid-range position for knowledge transfer, somewhere between the highest-level theory and the rather loose collection of practical actions under the 25 T organised by limited themes. The theory has been differentiated into the D principles and the actions consolidated into a smaller set of method categories (although to flesh out the toolkit, we devoted considerable effort to listing diverse exemplars under each category). Other such mid-range formulations might be considered worth developing in conveying the insights of Crime Science to practitioners; however, as the present project showed, this was no back-of-the-envelope affair but an extensive and intensive exercise involving researchers and practitioners.

Benefits to practitioners of using the modes of action

The modes of action which organise the D principles – Practical, Psychological and Personal – offer the broadest and most flexible way of contemplating interventions. But by the same token, with breadth and flexibility comes the downside of potential vagueness. This suggests, again, the presentation of exemplars, methods, principles and modes as alternatives to be continually switched between rather than a hierarchy of use. The modes bear some affinity to the Haddon Matrix (e.g. Haddon, 1980; see also Clarke and Newman 2006) for accidental injury prevention, which divides contributing factors into host, agent or vector and environment; and in a second dimension divides the process into pre-event, event and post-event phases. We note in passing that the second dimension could suggest that different modes, principles or methods could be suited to different phases. It could make a further useful connection with the finer-grained sequential focus of crime scripts.

Drawing on design

In some respects we have followed the spirit of the cumulative approach of SCP in evolving, adapting and extending thinking in the light of new theory, research and practice. The prime example is the extension of SCP techniques from 12 to 16 to 25. But we have done so with a more explicit design process.

Ekblom (2012a) argues that crime prevention practitioners should 'draw on design': i.e. think like designers and use design processes, rather than just use the end products of design. This maxim was reflected within the toolkit itself (namely, getting site security managers to 'think designer' at appropriate points). The crime scientists in the toolkit development team followed the maxim in their own approach too. The designers were not simply 'on tap' to provide good quality graphics but were fully involved from the start of the project. (A designer's view of the project is in Willcocks et al. 2012). They contributed to the common understanding as it evolved, giving valuable insights, raising challenges and thinking ahead to practical toolkit possibilities including maintaining a strong user focus. Their info-graphic representations, produced throughout the project, contributed to reflective practice and articulation of the wider team's emerging ideas. Their role in the iterative development of the Ds and the logic, workflow, illustration and text of the toolkit as a whole contributed greatly to the project as a whole. This is collaboration of a kind which should be contemplated in all crime prevention projects, whether capacity-building (as here), or operational.

Wider crime science benefits

The benefits of the principles/methods distinction to Crime Science itself are less straightforward to state. But we believe that articulating this particular 'Yin and Yang' relationship explicitly rather than tacitly can perhaps spark new research and theory simply by encouraging researchers to deliberately and systematically flip perspectives in a self-aware way.

We believe that there are particular benefits from the D principles too. Viewing our corpus of knowledge through a fresh facet, hence offering alternative, but rigorously and consistently linked, perspectives on the same theories and phenomena, can only stimulate thinking. Indeed, as we found, the very process of cutting and polishing new facets and trialling these on experienced and knowledgeable practitioners itself supplied and provoked new ideas.

In terms of the content of the Ds, we believe they should be applicable, with expansion perhaps, to the wider field of SCP. (Indeed, they were designed to apply to wider crime problems than terrorism in first place, in order to motivate security managers and their directors to use the hostile reconnaissance toolkit and apply its results. This greater scope would enable them to the benefit from preventing a larger number of less serious events than just extremely rare, but high-impact terrorist attacks.) In this, we see some payback, for generic SCP, of work originally undertaken with a counter-terrorism purpose: beginning with Roach et al. (2005) and Clarke and Newman (2006), the initial benefits flowed in the other direction. The relatively rare opportunity to carefully and selectively blend SCP/POP knowledge with ideas from the conventional security and enforcement world struck us as particularly fruitful. In fact, this reflects the aim of POP in bringing to bear *any*

and all disciplined approaches to tackle particular crime problems.

Implications for 25 T

So where does this leave the 25 Techniques? Our position is that they remain an excellent and versatile repository of structured practical knowledge for general purpose and introductory situational crime prevention. But there are circumstances such as in the present project, where situations to be addressed are highly diverse and the only common consideration is the adaptive and highly-motivated perpetrator. Here, approaches like the D principles focusing more sharply on more detailed offender-related but situational intervention mechanisms, may offer more flexible and more tailored structuring of knowledge, thinking and communication among practitioners, and between practitioners and researchers.

Ultimately, though, only deliberate evaluation will tell whether, following adoption of such approaches, the security actions generated by practitioners show consistent and significant increases in quantity and in quality. Such quality might be defined as problem- and context-appropriate, linked to what-works evidence and tested theory, and where necessary, innovative.

Strategic implications

In general, we believe researchers have become somewhat fixated on existing ways of organising Crime Science knowledge. Moreover there is a hesitancy to develop the science in ways that outstrip the capacity of practitioners to understand and use the knowledge (cf. Bouhana 2013). Clarke (2012) for example, argues for 'good enough theory'. But if we are to follow the Medical Science or Engineering Science models, these make a clear distinction between the advanced science, and what the various levels of practitioner (brain surgeon to paramedic; aircraft designer to garage mechanic) need to know of that science and how it is communicated. Though both must reside on the same wing, the trailing edge should not hold back the leading edge.

Endnotes

[a]We are grateful to a reviewer for this point.

Abbreviations

25 T: The 25 Techniques of Situational Crime Prevention; CCO: The conjunction of criminal opportunity; POP: Problem-oriented policing; SCP: Situational crime prevention.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

PE was the lead author but both authors contributed equally to the underlying research and thinking, with participation from acknowledged colleagues. Both authors read and approved the final manuscript.

Author information

PE is Professor of Design Against Crime at Central Saint Martins, University of the Arts London, and Visiting Professor at the University of Huddersfield and the Department of Security and Crime Science, UCL. AH is Professor of Criminology and Director of the Applied Criminology Centre at the University of Huddersfield and Visiting Professor at the Department of Security and Crime Science, UCL.

Acknowledgements

The authors are grateful to other project team members who included Rachel Armitage, Leanne Monchuk and Jason Roach (Huddersfield) and Marcus Willcocks, Rita Maldonado Branco and Lorraine Gamman (Central Saint Martins); also to those at CPNI (who funded the research and development), NaCTSO, various UK police forces and site security managers who gave us the opportunity to develop these ideas and contributed their own; and to peer reviewers and journal editors for useful feedback. The authors were funded out of salary and none of the latter groups instigated nor funded this publication.

Author details

[1]Design Against Crime Research Centre, Central Saint Martins, University of the Arts London, Granary Square, London N1C 4AA, UK. [2]Applied Criminology Centre, University of Huddersfield, Queensgate, Huddersfield HD1 3DH, UK.

Received: 3 October 2013 Accepted: 30 January 2014
Published online: 12 April 2014

References

Batschelet, A. (2002). *Effects-Based Operations: A New Operational Model? USAWC strategy research project*. Carlisle Barracks, PE: U.S. Army War College. www.iwar.org.uk/military/resources/effect-based-ops/ebo.pdf accessed 2.

Bouhana, N. (2013). The reasoning criminal vs. Homer Simpson: Conceptual challenges for crime science. *Front. Hum. Neurosci, 7*, 682. doi:10.3389/fnhum.2013.00682.

Clarke, R. (1999). *Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods* (Police Research Series 112). London: Home Office.

Clarke, R. (2008). Situational crime prevention. In R Wortley & L Mazerolle (Eds.), *Environmental Criminology and Crime Analysis*. Willan: Cullompton.

Clarke, R. (2012). Opportunity makes the thief. Really? And so what? *Crime Science, 1*, 3.

Clarke, R, & Eck, J. (2003). *Become a Problem Solving Crime Analyst in 55 Small Steps*. London: Jill Dando Institute, University College London.

Clarke, R, & Newman, G. (2006). *Outsmarting the Terrorists*. New York: Praeger Security International.

Cohen, L, & Felson, M. (1979). Social change and crime rate changes: a routine activities approach. *American Sociological Review, 44*, 588–608.

Cornish, D. (1994). *The procedural analysis of offending and its relevance for situational prevention. Crime Prevention Studies, 3*. Monsey: Criminal Justice Press.

Cornish, D, & Clarke, R. (1986). *The Reasoning Criminal*. New York: Springer-Verlag: Rational Choice Perspectives on Offending.

Eck, J. (2002). *Learning from experience in problem-oriented policing and situational prevention: The positive functions of weak evaluations and the negative functions of strong ones. Crime Prevention Studies, 14*. Monsey: Criminal Justice Press.

Ekblom, P. (2002). From the source to the mainstream is uphill: The challenge of transferring knowledge of crime prevention through replication, innovation and anticipation. In N Tilley (Ed.), *Analysis for Crime Prevention, Crime Prevention Studies* (pp. 13,131–203). Monsey, NY: Criminal Justice Press.

Ekblom, P. (2010). The conjunction of criminal opportunity theory. *Sage Encyclopedia of Victimology and Crime Prevention, 1*, 139–146.

Ekblom, P. (2011). *Crime Prevention, Security and Community Safety Using the 5Is Framework*. Basingstoke: Palgrave Macmillan see also. http://5isframework.wordpress.com accessed 1 October 2013.

Ekblom, P. (2012a). *Happy returns: Ideas brought back from situational crime prevention's exploration of design against crime. In G Farrell and N Tilley (Eds) The Reasoning Criminologist: Essays in Honour of Ronald V. Clarke, 163–98. Crime Science series*. Cullompton: Willan.

Ekblom, P. (2012b). *The security function framework. In P Ekblom (Ed.), Design Against Crime: Crime Proofing Everyday Objects. Crime Prevention Studies 27*. Boulder, CO: Lynne Rienner.

Ekblom, P, & Sidebottom, A. (2008). What do you mean, 'Is it secure?' Redesigning language to be fit for the task of assessing the security of domestic and personal electronic goods. *European Journal on Criminal Policy and Research, 14*, 61–87.
Felson, M. (1995). *Those who discourage crime. Crime Prevention Studies, 4*. Monsey, NY: Criminal Justice Press.
Haddon, W. (1980). Options for the prevention of motor vehicle crash injury. *Israeli Journal of Medical Science, 16*, 45–68.
Laycock, G. (2005). Defining crime science. In *Crime Science*. New Approaches to Preventing and Detecting Crime. Cullompton: Willan): M.J. Smith and N. Tilley.
Pawson, R, & Tilley, N. (1997). *Realistic Evaluation*. London: Sage.
Roach, J, Ekblom, P, & Flynn, R. (2005). The conjunction of terrorist opportunity: a framework for diagnosing and preventing acts of terrorism. *Security Journal, 18*, 7–25.
Scott, M, Eck, J, Knutsson, J, & Goldstein, H. (2008). Problem-oriented policing and environmental criminology. In R Wortley & L Mazerolle (Eds.), *Environmental Criminology and Crime Analysis*. Willan: Cullompton.
Tilley, N. (1993a). *After Kirkholt: Theory, Methods and Results of Replication Evaluations. Crime Prevention Unit Paper No. 47*. London: Home Office.
Tilley, N. (1993b). *Understanding Car Parks, Crime and CCTV: Evaluation Lessons from Safer Cities. Crime Prevention Unit Paper No. 42*. London: Home Office.
Tilley, N. (2006). *Knowing and doing: Guidance and good practice in crime prevention. In J Knutsson and R Clarke (Eds) Putting Theory to Work: Implementing Situational Prevention and Problem-Oriented Policing. Crime Prevention Studies 20*. Monsey, NY: Criminal Justice Press.
Wikström, P-O. (2007). *Doing without knowing: Common pitfalls in crime prevention. In G. Farrell, K. Bowers, S. Johnson and M. Townsley (Eds) Imagination for Crime Prevention: Essays in Honour of Ken Pease. Crime Prevention Studies, 21*. Monsey, NY: Criminal Justice Press.
Willcocks, M, Ekblom, P, & Hirschfield, A. (2012). *Co-designing a toolkit for controlling hostile reconnaissance. Open innovation in a controlled environment*. London, June: Presentation at International Crime Science Conference.
Wortley, R. (2008). Situational precipitators of crime. In R Wortley & L Mazerolle (Eds.), *Environmental Criminology and Crime Analysis*. Willan: Cullompton.
Wortley, R, & Mazerolle, L (Eds.). (2008). *Environmental Criminology and Crime Analysis*. Cullompton: Willan.

doi:10.1186/s40163-014-0002-5
Cite this article as: Ekblom and Hirschfield: **Developing an alternative formulation of SCP principles – the Ds (11 and counting).** *Crime Science* 2014 **3**:2.